AMENDMENTS TO THE CLAIMS

Applicant amends claims 1, 5, 6, 8, 12, 13, 17, 21, 22, 24, 28, 29, 31, and 32, as detailed below. This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) An information recording device comprising:

a memory unit containing data, including content data of a plurality of data files, a block permission table defining memory-access control information, and an integrity check value for the block permission table generated based on a memory unit identifier, the memory unit having a data storage area comprising a plurality of blocks, each block of the plurality of blocks comprising a plurality of [[M]] sectors ~~from a first sector to a M-th sector with~~ each sector of the plurality of sectors of each block of the plurality of blocks having a predetermined data capacity~~, where M represents a natural number~~;

a processing unit for dividing content data of each data file of the plurality of data files into separate content data portions, for storing, for each data file of the plurality data files, a first portion in a first sector of one of the plurality of blocks, and a second portion in a second sector of one of the plurality of blocks ~~each of the separate content data portions in a different sector within a first data block of the data storage area~~, and for storing a security header corresponding to the content data of the plurality of data files in at least one header block of the plurality of blocks, wherein the at least one header block is different from each one of the blocks in which the content data of the plurality of data files is stored ~~a second data block of the data storage area, wherein the first data block is different from the second data block~~;

a cryptosystem unit for performing sector level encryption by using a first ~~different~~ encryption key ~~for each sector of the first data block~~ to execute encryption of each first sector of each of the plurality of blocks, and using a second encryption key that is different from the first

encryption key to execute encryption of each second sector of each of the plurality of blocks ~~processing on the content data portion to be stored in each of the sectors~~; and

an integrity checking unit for checking the integrity of the block permission table based on the integrity check value generated based on the memory unit identifier,

wherein the security header stored in the ~~second data~~ header block includes each encryption key used for each sector of each of the plurality of blocks ~~the first data block~~.

2-4. (Cancelled).

5. (Currently Amended) An information recording device according to claim 1, wherein, in said cryptosystem unit, the encryption processing is executed as single-DES encryption processing using different encryption keys for each sector of the plurality of blocks ~~the first data block~~.

6. (Currently Amended) An information recording device according to claim 1, wherein, in said cryptosystem unit, the encryption processing is executed as triple-DES encryption processing using at least two different encryption keys for each sector of the plurality of blocks ~~the first data block~~.

7. (Cancelled).

8. (Currently Amended) An information playback device comprising:

a memory unit containing data, including encrypted content data, a block permission table defining memory-access content data of a plurality of data files, and an integrity check

value for the block permission table generated based on a memory unit identifier, the memory unit having a data storage area comprising a plurality of blocks, each block of the plurality of blocks comprising a plurality of [[M]] sectors ~~from a first sector to a M-th sector with~~ each sector of the plurality of sectors of each block of the plurality of blocks having a predetermined data capacity~~, where M represents a natural number~~;

a processing unit for reading encrypted content data portions which together comprise encrypted content data of the plurality of data files, wherein, for each data file of the plurality data files, a first portion is read from a first sector of one of the plurality of blocks, and a second portion is read from a second sector of one of the plurality of blocks, and wherein each first sector of each of the plurality of blocks is encrypted using a first encryption key, and each second sector of each of the plurality of blocks is encrypted using a second encryption key that is different from the first encryption key, ~~each encrypted content data portion has been encrypted using a different encryption key and is read from a different sector within a first data block of the data storage area~~, and for reading a security header corresponding to the encrypted content data of the plurality of data files from at least one header block of the plurality of blocks, wherein the at least one header block is different from each one of the blocks in which the content data of the plurality of data files is stored ~~from a second data block of the storage area, wherein the first data block is different from the second data block~~;

a cryptosystem unit for performing sector level decryption by using a first decryption key to decrypt data read from the first sector of each of the plurality of blocks and using a second decryption key that is different from the first decryption key to decrypt data read from the second sector of each of the plurality of blocks, ~~a different decryption key for each sector of the first data block to execute decryption processing on the read encrypted content data portions~~; and

an integrity checking unit for checking the integrity of the block permission table based on the integrity check value generated based on the memory unit identifier,

wherein the security header read from the ~~second data~~ header block includes each encryption key used to encrypt each encrypted content data portion read from each of the plurality of blocks ~~the first data block~~.

9-11. (Cancelled).

12. (Currently Amended) An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing is executed as single-DES decryption processing using different decryption keys for each sector the plurality of blocks ~~the first data block~~.

13. (Currently Amended) An information playback device according to claim 8, wherein, in said cryptosystem unit, the decryption processing is executed as triple-DES decryption processing using at least two different decryption keys for each sector of the plurality of blocks ~~the first data block~~.

14-16. (Cancelled).

17. (Currently Amended) An information recording method comprising the following steps performed by a control unit:

dividing content data of a plurality of data files into separate content data portions;

storing the separate content data portions, a block permission table defining memory-access control information, and an integrity check value for the block permission table generated based on a medium identifier, to a memory medium having a data storage area comprising a plurality of blocks, each block of the plurality of blocks comprising a plurality of [[M]] sectors ~~from a first sector to a M-th sector with~~ each sector of the plurality of sectors of each block of the plurality of blocks having a predetermined data capacity~~, where M represents a natural number~~, for each data file of the plurality data files, a first portion is stored in a first sector of one of the plurality of blocks, a second portion is stored in a second sector of one of the plurality of blocks, and a security header corresponding to the content data of the plurality of data files is stored in at least one header block of the plurality of blocks that is different from each one of the blocks in which the content data of the plurality of data files is stored ~~each content data portion is stored in a different sector within a first data block of the data storage area and the security header is stored in a second data block of the data storage area, wherein the first data block is different from the second data block~~;

encrypting, prior to storing, the content data portions by performing sector level encryption using a first encryption key to execute encryption of each first sector of each of the plurality of blocks, and using a second encryption key that is different from the first encryption key to execute encryption of each second sector of each of the plurality of blocks ~~a different encryption key for each sector of the first data block in which a content data portion will be stored~~; and

performing an integrity check of the block permission table based on the integrity check value generated based on the medium identifier,

wherein the security header stored in the ~~second data~~ header block includes each encryption key used to encrypt each content data portion stored in the sectors of the plurality of blocks ~~the first data block~~.

18-20. (Cancelled).

21. (Currently Amended) An information recording method according to claim 17, wherein encrypting is executed as single-DES encryption processing using different encryption keys each sector of the plurality of blocks ~~the first data block~~.

22. (Currently Amended) An information recording method according to claim 17, wherein encrypting is executed as triple-DES encryption processing using at least two different encryption keys for each sector of the plurality of blocks ~~the first data block~~.

23. (Cancelled).

24. (Currently Amended) An information playback method comprising the following steps performed by a control unit:

reading encrypted content data portions, which together comprise encrypted content data of a plurality of data files, a block permission table defining memory-access control information, an integrity check value for the block permission table generated based on a medium identifier, and a security header from a memory medium having a data storage area comprising a plurality of blocks, each block of the plurality of blocks comprising a plurality of [[M]] sectors ~~from a first sector to a M-th sector with~~ each sector of the plurality of sectors of each block of the

plurality of blocks having a predetermined data capacity~~, where M represents a natural number~~, wherein, for each data file of the plurality data files, a first portion is read from a first sector of one of the plurality of blocks, and a second portion is read from a second sector of one of the plurality of blocks, and wherein each first sector of each of the plurality of blocks is encrypted using a first encryption key, and each second sector of each of the plurality of blocks is encrypted using a second encryption key that is different from the first encryption key, and the security header, corresponding to the encrypted content data of the plurality of data files, is read from at least one header block of the plurality of blocks, wherein the at least one header block is different from each one of the blocks in which the content data of the plurality of data files is stored ~~each encrypted content data portion having been encrypted using a different encryption key and read from a different sector within a first data block of the data storage area, and the security header read from a second data block of the data storage area, wherein the first data block is different from the second data block~~;

decrypting the content data portions stored in each of the sectors by performing sector level decryption by using a first decryption key to decrypt data read from the first sector of each of the plurality of blocks and using a second decryption key that is different from the first decryption key to decrypt data read from the second sector of each of the plurality of blocks ~~using a different decryption key for each sector of the first data block to execute decryption processing on the read encrypted content data portions~~; and

performing an integrity check of the block permission table based on the integrity check value generated based on the medium identifier,

wherein the security header read from the ~~second data~~ header block includes each encryption key used to encrypt each encrypted content data portion read from each of the plurality of blocks ~~the first data block~~.

25-27. (Cancelled).

28. (Currently Amended) An information playback method according to claim 24, wherein the decryption processing is executed as single-DES decryption processing using different decryption keys each sector of the plurality of blocks ~~the first data block~~.

29. (Currently Amended) An information playback method according to claim 24, wherein the decryption processing is executed as triple-DES decryption processing using at least two decryption keys for each sector of the plurality of blocks ~~the first data block~~.

30. (Cancelled).

31. (Currently Amended) A computer-readable recording medium comprising a computer program product for performing, when executed by a processor, a data encryption method comprising:

dividing content data of a plurality of data files into separate content data portions;

storing the separate content data portions, a block permission table, an integrity check value for the block permission table generated based on a memory unit identifier, and a security header in a memory unit having a data storage area comprising a plurality of blocks, each block of the plurality of blocks comprising a plurality of [[M]] sectors ~~from a first sector to a M-th sector with~~ each sector of the plurality of sectors of each block of the plurality of blocks having a predetermined data capacity~~, where M represents a natural number~~, for each data file of the plurality data files, a first portion is stored in a first sector of one of the plurality of blocks, a

second portion is stored in a second sector of one of the plurality of blocks, and a security header corresponding to the content data of the plurality of data files is stored in at least one header block of the plurality of blocks that is different from each one of the blocks in which the content data of the plurality of data files is stored ~~each content data portion being stored in a different sector within a first data block of the data storage area and the security header being stored in a second data block of the data storage area, wherein the first data block is different from the second data block~~;

encrypting, prior to storing, the content data portions by performing sector level encryption using a first encryption key to execute encryption of each first sector of each of the plurality of blocks, and using a second encryption key that is different from the first encryption key to execute encryption of each second sector of each of the plurality of blocks ~~a different encryption key for each sector of the first data block in which a content data portion will be stored~~; and

checking the integrity of the revocation list and the block permission table based on the integrity check value generated based on the memory unit identifier,

wherein the security header stored in the ~~second data~~ header block includes each encryption key used for each sector of the plurality of blocks ~~the first data block~~.

32. (Currently Amended) A computer readable recording medium comprising a computer program product for performing, when executed by a processor, a data decryption method comprising:

reading encrypted content data portions, which together comprise encrypted content data of a plurality of data files, a block permission table defining memory-access control information, an integrity check value for the block permission table generated based on a memory identifier,

and a security header from a memory having a data storage area comprising a plurality of blocks, each block of the plurality of blocks comprising a plurality of [[M]] sectors ~~from a first sector to a M-th sector with~~ each sector of the plurality of sectors of each block of the plurality of blocks having a predetermined data capacity~~, where M represents a natural number~~, wherein, for each data file of the plurality data files, a first portion is read from a first sector of one of the plurality of blocks, and a second portion is read from a second sector of one of the plurality of blocks, and wherein each first sector of each of the plurality of blocks is encrypted using a first encryption key, and each second sector of each of the plurality of blocks is encrypted using a second encryption key that is different from the first encryption key, and the security header, corresponding to the encrypted content data of the plurality of data files, is read from at least one header block of the plurality of blocks, wherein the at least one header block is different from each one of the blocks in which the content data of the plurality of data files is stored ~~each encrypted content data portion having been encrypted using a different encryption key and read from a different sector within a first data block of the data storage area, and the security header read from a second data block of the data storage area, wherein the first data block is different from the second data block~~;

decrypting the content data portions stored in each of the sectors by performing sector level decryption by using a first decryption key to decrypt data read from the first sector of each of the plurality of blocks and using a second decryption key that is different from the first decryption key to decrypt data read from the second sector of each of the plurality of blocks ~~using a different decryption key for each sector of the first data block to execute decryption processing on the read encrypted content data portions~~; and

checking the integrity of the block permission table based on the integrity check value generated based on the memory identifier,

wherein the security header read from the ~~second data~~ header block includes each encryption key used to encrypt each encrypted content data portion read from each of the plurality of blocks ~~the first data block~~.